Group 23

Participants — Michael Schwob, Brandon Weinerman, Jorja Szczerbinski, Nazman Rosman, Taylor Smith, Donald Wheeler

Non-Participants – N/A

Date – 20 November 2024

GA Part 5: Analysis and Synthesis Paper

Introduction

The U.S. Health Sector Cybersecurity Coordination Center (HC3) issued a report alerting the U.S. health sector of hacker group Killnet, which targets domestic healthcare facilities with cyber-attacks. Killnet is a Russian nationalist organization that is primarily motivated to support Russia by attacking Ukraine and Western allies like the United States. The main threat that Killnet poses is the distributed denial-of-service attacks that it employs to cause serious disruption to the services of healthcare institutions (American Hospital Association, 2023). These service interruptions could end up costing the well-being or even lives of patients. Killnet also works to breach organizational networks to compromise sensitive healthcare information. The U.S. Department of Health and Human Services and healthcare facilities must work together to strengthen the cybersecurity posture of the U.S. health sector so that the health and privacy of patients can be protected. Additional resources will need to be diverted to IT infrastructure such as web application firewalls and DDoS filtering systems, but this should be a priority as the U.S. healthcare sector becomes increasingly more dependent on IT functions.

Overview of Critical Infrastructure

The CI that we chose is healthcare. The event we chose to focus on was the DDoS attacks done by the hacker group Killnet. This group of hackers sought out multiple attacks upon various healthcare services mainly in western countries. They could attack multiple services because their first attack was on an organization that supported the military, which then led to them growing a lot as a group. Additionally, using DDoS allowed them to have a low-cost way of disrupting the online websites and services being used but still drawing a lot of attention to them. These attacks are anonymous, which makes it difficult for them to be tracked down. The attacks mostly happened over the platform Azure, which is a computing platform that operates in several data centers. Observing Killnet's attacks, they started off with around 10-20, which then grew rapidly to around 40-60 in a three-month period. (Dahan, Pasha, 2023) They were attacking these places that had little to no security on their websites. To try and not get caught, they used different attack patterns to try and keep their identity hidden. Their different attack patterns consisted of switching it between layer 4 and 7 techniques of attack, while adding more sources doing the attacks as well. For the future, there are several things you can do to not have this happen. The first step you can take is enabling the network protection for the DDoS. By doing

this you are minimizing the threat and risk of getting hacked. Two other ways you can help yourself are to reach out for help if you do get attacked and know what to do after it happens. Reaching out and letting an expert know can help stop the attackers from doing it to more people. This event is to be considered as foreign terrorism.

Primary Assets, Protector & Threat

In the scope of our analysis, the primary asset identified is the preservation of patient lives. The health care sector's main purpose is to protect and care for patients as they receive treatment and go through recovery for illness or injury. Protecting patients' privacy is of utmost importance in any healthcare system. To build and upkeep a dependable and distinguished reputation patients must feel inclined to put their trust in the hands of the healthcare facility that could be responsible for their lives when they are the most vulnerable.

IT equipment and the security of their systems is essential to allowing healthcare facilities to operate smoothly. For this reason, the IT infrastructure of healthcare facilities is an essential protector for the health care sector. Weakened web servers and cyber security allow easy access for potential threats to harm the healthcare sector. The key threat of our analysis deals with a series of DDoS attacks sent by Killnet's hacktivists. This organization has targeted various healthcare facilities, preying on their weaknesses, and flooding web servers that are ill-prepared for these unanticipated attacks. Cyber-attacks on healthcare facilities can cause time consuming disruptions, which can make it difficult to provide life-saving care that patients need (Shamus, 2023, Pg. 1). For many hacktivists launching DDoS attacks, the goal is to blackmail its

Links to other CI's

Besides healthcare, this cyberterrorist attack impacted other CIs, namely the communications sector and the information technology sector. As explained earlier, the DDoS attacks caused major outages of healthcare systems throughout the country, and these healthcare systems are responsible for handling communication between doctors, nurses, and patients as well as storing sensitive patient information. When the system was made inaccessible by the attackers, the standard method of communications between patients and healthcare providers therefore became unavailable. Consequently, patients may resort to using less secure mediums of

communication such as email and phone to contact their providers, increasing the risk of compromising their privacy. Next, the information technology infrastructure was sabotaged when crucial patient information became unavailable due to the attack. Most medical processes, such as patient assessment, diagnosis, treatment planning, and monitoring, require doctors to refer to patient information on the system. Disruption in healthcare systems can also disrupt these medical processes, potentially leading to severe consequences, including the loss of life.

Related World Events

The most significant event that influenced Killnet's attacks on the Healthcare Sector was the war between Russia and Ukraine. The birth of the Killnet organization coincided with increasing tensions between Russia and Ukraine, as Ukraine continued strengthening ties with Western countries and NATO. Russia invaded Ukraine the very next month after Killnet was established, in February 2022. Killnet chose its targets based on who was providing aid to Ukraine and criticizing Russia. The U.S., being the most powerful and influential country in NATO and a strong ally to Ukraine, was therefore a natural target for Killnet.

The Healthcare sector was already in a vulnerable state in 2022 when the attacks began, owing to the global pandemic of the COVID-19 virus that swept the world in early 2020. This virus had massive effects on healthcare sectors across the globe, and the U.S. was no exception. Healthcare institutions were extremely drained during this time and had more immediately pressing problems than cybersecurity. Healthcare sector saw major disruptions to services with the National Library of Medicine citing issues such as "shifting of health care workers to support COVID-19 services, cancellations of planned treatments, decrease in public transport, loss of income to pay for services and limit utilization" (Haileamlak, 2021). Healthcare organizations needed to respond by diverting many resources towards dealing with the deadly virus. This in turn substantially limited the resources that could be directed towards IT infrastructure and staff. Killnet was able to take advantage of the subpar cybersecurity posture many health facilities had resulting in part from the strain brought on by the pandemic.

A world event that limited the threat of Killnet to the U.S. health sector was the creation of rules for cyber-warfare by the International Committee of the Red Cross (ICRC) in October 2023. The eight rules created were intended to protect civilians of all countries from becoming victims to the harmful disruptions caused by cybercrimes. Both Killnet and the IT Army of Ukraine agreed to these rules, leading to a drop in cyberattacks from both groups (Tidy, 2023).

Killnet since seems to be shifting from a hacktivist group motivated by primarily Russian nationalism to a group more focused on financial gain. Killnet has transitioned to using phishing and ransomware attack more, methods that are increasingly popular for hacker groups with financial motives (Al-Aboosi et al., 2023). They seem to no longer publicly target pro-Ukrainian countries like the U.S. and instead sell their hacking services to others (Flashpoint, n.d.).

Intelligence Strategies

There are a variety of intelligence collection methods that could be used in this case, one being Red Cell Analysis and another being the use of the "INTS," more specifically "SIGINT." Red Cell Analysis is the idea of predicting someone's behavior by putting yourself in their shoes, which is something we could do to predict how the attackers will try to "break in." Signals Intelligence (SIGINT) is gathered from data transmissions, which include communications intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). We can use these tools to find out where the hackers reside, who they are, and how they are trying to break into our cyberspace.

Red Cell Analysis is an extremely valuable tool in our case, as you must think like a hacker to understand how and when they are planning to break into secure systems. Using this technique allows healthcare companies to test their systems, looking for any weak points before the hackers do. This technique also allows the companies to better understand what the hacker's intentions/goals are and what information they are interested in. They might also consider using a new software/protection service to mitigate the risk of being attacked. Microsoft tested its own Azure software to see if it was successful at defending the site. Microsoft's Azure DDos Network Protection claims, "Customers can defend themselves against even the most sophisticated attacks with an Azure global network that provides dedicated monitoring, logging, telemetry, and alerts." (Dahan, 2023). After somewhat "reverse engineering" the DDos attacks, they were successful in building a new software to better protect many of these healthcare services.

Another intelligence communication method that is extremely useful in this case is Signals Intelligence (SIGINT), which is one of the Intelligence Collection Disciplines (INTS). SIGINT is defined as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems that provides a

vital window for our nation into foreign adversaries' capabilities, actions, and intentions." (NSA). This method is very valuable as it helps to determine who the offender is, where they are, and what information they have exchanged with others. It is extremely challenging to prevent situations like this unless the offender is identified and surveilled. Using this method, there is a possibility to intercept information between offenders, which will act as a warning for healthcare services and their security sector. Additionally, intercepted information will advise security services of what specific steps they are taking to gain access to information.

Reducing Analysis & Recommendations

The likelihood of DDoS attacks from striking our hospitals and doctor offices is exceedingly high in our future. The dependence of technology in hospitals will continue to make it a big target for organizations like Killnet. It was said that in 2024 there was "an average of 1,876 per organization recorded". (Check Point Team). That was a 75% increase compared to 2023, and it will continue to grow, unless we have a plan to stop it.

Our group's idea to prevent these DDoS attacks is to protect and strengthen our IT equipment by adding Anycast networks and limiting our outside traffic use on all devices. What we mean by limiting outside traffic use is by keeping our devices catered towards our work. Whether that means we block all outside sites and databases like different emails, search engines and websites. It will keep our data and information provided on one locked screen. For example, blocking out separate emails and remaining on the pages only used for the healthcare workers needed will not allow for us to be reached by DDoS attacks if we are not on them in the first place. With the addition of the anycast network it can absorb and control the traffic spikes and broadens the surface of it in general. This makes it hard for the floods that DDoS attacks have on our devices to truly take over and break it down. Making our surface bigger will result in DDoS not breaking down our computer and still being able to function it.

The pros to blocking outside cites and limiting our access with the addition of anycast networks is that it will protect patients' data and information, resulting in them feeling more

comfortable with their privacy in our devices. By preventing these attacks, it will limit the money we have to spend to fix our IT after an attack. Finally upgrades of the technology will allow for healthcare workers to operate more smoothly and efficiently. Cons can consist of having to train and spend money on employees to learn to operate and install the networks and proper technology to prevent attacks. It does not guarantee protection against DDoS, and use of it with weak passwords, poor methods and out of date software may leave devices more vulnerable to attacks. With that being said, a way to mitigate these attacks would be to install different firewalls and server networks to handle/protect. With the installation of certain networks and servers it will not stop the DDoS attack from happening but upon detection it can "vacuum" the attacks and block the flooding from happening. For example, with the installation of VAC, it is a server that works on our computers to detect when an attack is coming and "vacuum" up the flooding, it will then block it from entering and dismantling our device. This is called auto-mitigation which is by OVHCloud.

Pros to the "vacuum" strategy are that it is a non-manual factor to mitigate the risk of these attacks from coming. It also allows us to function on our device while the attack is going on, not slowing down, and messing with the efficiency in our hospitals. Cons on the other hand are that it all depends on the DDoS attacks, that there are several different attacks that can be sent, and it cannot stop all of them. If a hacker group like Killnet becomes aware of the mitigation strategies, they will be able to work their way around the server. And finally with technology growing this method may soon be outdated, and it will likely become useless to stop these attacks someday because of advances in other technology.

Conclusion

In conclusion, the attacks of Killnet affected tons of people. Taking away from this, having secure and protected websites is crucial moving forward so that something like this doesn't happen again. Adding things like firewalls is just one way of getting more security. If more healthcare services had been attacked, more people would have been exposed and at risk.

Bibliography

Al-Aboosi, A. M. M., Abdullah, S. N. H. S., Murah, M. Z., & Dharhani, G. S. A. (2022, October 6-7). Cybersecurity Trends in Health Information Systems. 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates. https://ieeexplore-ieee-org.ezaccess.libraries.psu.edu/document/9995952

American Hospital Association. (2023, January 30). *HC3 TLP clear analyst note: Pro-Russian hacktivist group threat to HPH sector January 30, 2023: AHA*. https://www.aha.org/cybersecurity-government-intelligence-reports/2023-01-30-hc3-tlp-clear-analyst-note-pro-russian-hacktivist-group-threat-hph

Cloudflare. (n.d.). *How to prevent ddos attacks | methods and tools.* Cloudflare. https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

Dahan, A., & Pasha, S. (2023, March 17). KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/?msockid=27462cbff24a6244001c3859f338636d

Flashpoint. (n.d.). Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective. Flashpoint. https://flashpoint.io/intelligence-101/killnet/

Forescout. (n.d.). *Killnet: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group*. Forescout Vedere Labs. https://www.forescout.com/resources/analysis-of-killnet-report/

Gmcdouga. (2024a, October 17). *A closer look at Q3 2024: 75% surge in cyber attacks worldwide*. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/#:~:text=A%20Record%20Spike%20in%20Attacks,rise%20from%20the%20previous%20quarter.

Hall, C. (2023, Feb 01). *U-M health websites attacked*. Livingston County Daily Press & Argus Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/newspapers/u-m-health-websites-attacked/docview/2771236817/se-2

Haileamlak, A. (2021, November 31). *The impact of COVID-19 on health and health systems*. National Library of Medicine. https://pmc.ncbi.nlm.nih.gov/articles/PMC8968362/

Kristen, J. S. (2023, Sep 06). Increase in cyberattacks at hospitals worrisome. *Battle Creek Enquirer* Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/newspapers/increase-cyberattacks-at-hospitals-worrisome/docview/2861047842/se-2

Li C, Wu Y, Yuan X, et al. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. *Int J Commun Syst*. 2018; 31:e3497. https://doi-org.ezaccess.libraries.psu.edu/10.1002/dac.3497

Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., & Yongchareon, S. (2024). Health iot threats: Survey of risks and vulnerabilities. *Future Internet*, *16*(11). https://doi.org/10.3390/fi16110389

Mohsin, A. S. M., & Muyeed, M. A. (2024). IoT based smart emergency response system (SERS) for monitoring vehicles, home, and health status. Discover Internet of Things, 4(1), 22. doi:https://doi.org/10.1007/s43926-024-00073-6

OVHcloud. (n.d.). *How to stop ddos attacks?*. OVHcloud. https://us.ovhcloud.com/security/anti-ddos/how-stop-ddos-steps/#:~:text=Once%20an%20attack%20is%20detected,flow%20and%20reach%20the%20server.

Rojas, A. (2023, Jan 31). *University of Iowa hospitals and clinics websites face outages after cyberattack.* University Wire Retrieved from https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/wire-feeds/university-iowa-hospitals-clinics-websites-face/docview/2771168644/se-2

Tidy, J. (2023, April 5). *KillNet's Targeting of the Health and Public Health Sector (December 2022 – March 2023)*. U.S. Department of Health and Human Services. https://www.bbc.com/news/technology-67029296

Tidy, J. (2023, October 6). *Ukraine cyber-conflict: Hacking gangs vow to de-escalate*. BBC News. https://www.bbc.com/news/technology-67029296

National Security Agency. "National Security Agency/Central Security Service > Signals Intelligence > Overview." *Www.nsa.gov*, 2024, www.nsa.gov/Signals-Intelligence/Overview/.